QUALITY ENGINEERING FOR THE IOT

Axel Rennoch, Sascha Hackel
TestingStage, Kiev, April 13, 2018
BERLIN CENTER FOR DIGITAL TRANSFORMATION

Digital Transformation from A to Z

Transfer Centers:
- IoT
- 5G Testbed
- Industrie 4.0
- Hardware for CPS Lab

Experience
Learning
Consulting
Development
Testing
Solutions

lab tours
digital strategy
qualification & training
workshops
business models
technology advisory
modeling
pilot solutions
implementation
engineering
system integration
software licensing

testing & QC

Industry Forum
• IoT test objects, goals, and configuration

• IoT test automation
  – IoT test language TTCN-3
  – IoT-Testware project

• IoT-T testlab

• IoT-Quality Engineering outlook
Where are we?
MOTIVATION – DEFINITION IOT

An *infrastructure* of interconnected *objects, people, systems and information resources* **together with** intelligent *services* to allow them to process information of the physical and the virtual world and react.

(ISO JTC 1/SWG 5 July 29-31, 2014)
MOTIVATION FOR QUALITY

• Mirai botnet, October 2016:
  – botnet using **insecure configured** IoT-devices
  – attack causes **blackout** and **disruption**
    (e.g. Amazon, Netflix, Twitter, Github)

• Wannacry, May 2017: cyber attack on steel mill in Germany, …

• KRACK (Key Reinstallation Attack), October 2017:
  Replay attack on Wi-Fi Protected Access protocol (WPA2), …

• Spectre and Meltdown, January 2018
  – Spectre: vulnerability that perform branch prediction in modern microprocessors
  – Meltdown: hardware vulnerability that allows to read all memory
TRENDS IN IOT

TOP IOT CONCERNS

CONNECTIVITY PROTOCOLS

MESSAGING STANDARDS

What messaging protocol(s) do you use for your IoT solution?

- HTTP: 60.1%
- MQTT: 54.7%
- CoAP: 26.7%
- In-house / proprietary: 18.4%
- HTTP/2: 16.8%
- AMQP: 15.0%
- XMPP: 10.3%
- Other: 7.1%
- Don't know: 7.1%
- Proprietary vendor protocol (specify below): 4.9%
- DDS: 4.0%
- None: 3.6%

67.0% 66.4% 54.0% 2%

IoT Developer Survey 2017 - Copyright Eclipse Foundation, Inc.
### CHALLENGES IN IOT

- **Wide portfolio of competences required**
  - Devices (sensors, HW, embedded SW)
  - Platforms (Cloud, platform domain knowledge)
  - Applications (SW, dashboard, business logic)

- **IoT platforms**
  - 360+ worldwide

- **IoT protocols**
  - Rich selection
  - IP-based
  - non-IP based

- **Connectivity options**
  - Throughput
  - Latency
  - Power efficiency
  - Packet size

---

#### IoT application logic

<table>
<thead>
<tr>
<th>Connectivity options</th>
<th>Services</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cellular: 4G, NB-IoT, Cat-M1, EC-GSM...[5G]; non-cellular: Wifi, LoRa, Sigfox, Zigbee, BLE...</td>
<td>IoT services layer</td>
<td>IoT application logic</td>
</tr>
<tr>
<td>Cellular netw.</td>
<td>CoAP</td>
<td></td>
</tr>
</tbody>
</table>

- **Cellular**
  - 4G, NB-IoT, Cat-M1, EC-GSM...[5G]
  - Non-cellular: Wifi, LoRa, Sigfox, Zigbee, BLE, ...

- **CoAP**
  - DTLS
  - DTLS
  - TLS/SSL

- **TCP**
  - UDP

- **IPv4/IPv6(6loWPAN)**

---

- **HTTP**
  - Web Socket
  - AMQP

- **XMPP**
  - MQTT
  - MQTT-SN

- **CoAP**
  - DTLS
  - DTLS
  - TLS/SSL

- **UDP**
  - SMS

- **IPv4/IPv6(6loWPAN)**

---

- **Cellular**
  - 4G, NB-IoT, Cat-M1, EC-GSM...[5G]
  - Non-cellular: Wifi, LoRa, Sigfox, Zigbee, BLE, ...

---

- **Cellular netw.**
QUO VADIS IOT?

Cathedral OR Bazaar?
STARTING: TEST OBJECTS

- **IoT devices**,  
  - Mikrocontroller *(MCU)*,  
  - **Gateways** (Bosch XDK, IoT starterkits)
- **IoT platforms**  
  - RIOT, relayr, Thread, mbed…  
  - service layer (oneM2M, FiWare)
- **IoT protocols**  
  - Constrained Application Protocol *(CoAP)*  
  - MQ Telemetry Transport *(MQTT)*

**IoT challenges**: complexity, asynchronism, long operation phase, resource constraints
LONG OPERATION LIFETIME

- After the acceptance and system tests there will be a long operation phase => new test phase „operation“
- Some parts of the IoT solution may be inaccessible (updated during the operation phases)
INTEGRATION OF SEVERAL TESTING APPROACHES

IoT Testing

- Software Testing
- System Testing
- Protocol Testing
- Security Testing
- Test Automation
TEST AUTOMATION

• Less **resources** needed (time and money)

• **Avoid** human **mistakes** due to manually testing

• During test **development and execution**

• **Speed-up** of **regression** tests and product **time-to-market**
MULTIPLE TEST CONFIGURATION (SAMPLES)
• **Toolset** *(selection of available means)*

  - **Protocol tester/monitor** *(Eclipse Titan, Wireshark)*
  - **Test devices** *(RFID kit, Bluetooth test device)*
  - **GUI tester** *(Selenium, SikuliX, Chrome headless)*
  - **Web services tester** *(soapUI)*

  ...

• **Public Testsuites** *(in preparation)*
  – Application of a standardized notation
  – Abstract and platform-independent
IOT TEST LANGUAGE

Did you know that your phone...

...has been tested using ETSI specifications written in TTN3?
TTCN-3 is the **Testing and Test Control Notation**

Internationally standardized testing language for formally defining test scenarios.

Designed **purely for testing**

```tcc
testcase Hello_Bob () {
    p.send("How do you do?");
    alt {
        []p.receive("Fine!") {
            setverdict( pass );
        }
        [else] {
            setverdict( inconc ) //Bob asleep!
        }
    }
}
```
CONTRIBUTION TO IOT TESTING

What else?

Fraunhofer FOKUS

TESTING STAGE '18

Engineering a Connected World
THE CONTEXT

Projects

Eclipse IoT open source projects help you build IoT Devices, Gateways ("Smart Objects"), Cloud backends, and more.
Use the list below to find the project that's right for you.

Eclipse Paho

The Paho project provides reliable open-source implementations of open and standard messaging protocols aimed at new, existing, and emerging applications for Machine-to-Machine (M2M) and Internet of Things (IoT). Paho reflects the inherent physical E.T...
THE ECLIPSE PROJECT

• Supplement to **running** Eclipse projects
  – Paho, OM2M, Titan

• **New project** at Eclipse Foundation:
  [https://projects.eclipse.org/projects/technology.iottestware](https://projects.eclipse.org/projects/technology.iottestware)
  – TTCN-3 test suites for **CoAP, MQTT, OPC-UA**, LoRa?

• Assured **licenses** for users

• **Currently in cooperation with**
  relayr GmbH, Ericsson, LAAS/CNRS, itemis AG, Spirent Communications,
  Easy Global Market, Iskratel/Sintesio, …
This proposal has been approved and the Eclipse IoT-Testware project has been created.
SAMPLE TESTSUITE STRUCTURE: MQTT

- Broker as SUT
  - All mandatory message data fields
    - Regular and illegal data
      (Fixed/variable header, payload)
  - Protocol features
    - General
    - Connect/disconnect (session)
    - Subscribe/unsubscribe
    - Immediate publish
    - Last will and Testament (LWT)
    - Heartbeats keepAlive values
    - Topic
    - Error handling
- Client as SUT
  - …
TEST DEVELOPMENT SAMPLE: MQTT

✓ Test configurations

✓ Test Suite Structure

✓ Test purpose (catalogue)

✓ Test implementation (TTCN-3)

<table>
<thead>
<tr>
<th>TP-ID</th>
<th>TP_MQTT_Broker_CONNECT_001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selection</td>
<td>PIC_Broker</td>
</tr>
<tr>
<td>Summary</td>
<td>The IUT MUST close the network connection if fixed header flags in CONNECT Control Packet are invalid</td>
</tr>
<tr>
<td>Reference</td>
<td>[MQTT-2.2.2-1], [MQTT-2.2.2-2], [MQTT-3.1.4-1], [MQTT-3.2.2-6]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Initial condition</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Test purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that the IUT on receipt of an CONNECT message containing header_flags := ’1111’B sends no RESPONSE message and closes the Network Connection</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Comments</th>
</tr>
</thead>
</table>
## MQTT BROKER EVALUATION (JULY 2017)

<table>
<thead>
<tr>
<th>Broker</th>
<th>Version</th>
<th>PASS #</th>
<th>PASS %</th>
<th>FAIL #</th>
<th>FAIL %</th>
<th>INCONCLUSIVE #</th>
<th>INCONCLUSIVE %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mosquitto</td>
<td>1.4.14</td>
<td>40</td>
<td>88.89%</td>
<td>3</td>
<td>6.67%</td>
<td>2</td>
<td>4.44%</td>
</tr>
<tr>
<td>VerneMQ</td>
<td>1.1.0</td>
<td>39</td>
<td>86.67%</td>
<td>3</td>
<td>6.67%</td>
<td>3</td>
<td>6.67%</td>
</tr>
<tr>
<td>HiveMQ</td>
<td>broker.hivemq.org</td>
<td>39</td>
<td>86.67%</td>
<td>4</td>
<td>8.89%</td>
<td>2</td>
<td>4.44%</td>
</tr>
<tr>
<td>EMQ</td>
<td>2.0</td>
<td>36</td>
<td>80.00%</td>
<td>7</td>
<td>15.56%</td>
<td>2</td>
<td>4.44%</td>
</tr>
<tr>
<td>lannister</td>
<td>?</td>
<td>31</td>
<td>68.89%</td>
<td>12</td>
<td>26.67%</td>
<td>2</td>
<td>4.44%</td>
</tr>
<tr>
<td>ActiveMQ</td>
<td>5.14.5</td>
<td>31</td>
<td>68.89%</td>
<td>12</td>
<td>26.67%</td>
<td>2</td>
<td>4.44%</td>
</tr>
<tr>
<td>RSMB</td>
<td>?</td>
<td>26</td>
<td>57.78%</td>
<td>17</td>
<td>37.78%</td>
<td>2</td>
<td>4.44%</td>
</tr>
<tr>
<td>RabbitMQ</td>
<td>3.5.7</td>
<td>21</td>
<td>46.67%</td>
<td>24</td>
<td>53.33%</td>
<td>0</td>
<td>0.00%</td>
</tr>
<tr>
<td>Mosca</td>
<td>2.5.1</td>
<td>19</td>
<td>42.22%</td>
<td>24</td>
<td>53.33%</td>
<td>2</td>
<td>4.44%</td>
</tr>
<tr>
<td>Moquette</td>
<td>0.10</td>
<td>16</td>
<td>35.56%</td>
<td>29</td>
<td>64.44%</td>
<td>0</td>
<td>0.00%</td>
</tr>
<tr>
<td>HBMQTT</td>
<td>0.9</td>
<td>15</td>
<td>33.33%</td>
<td>30</td>
<td>66.67%</td>
<td>0</td>
<td>0.00%</td>
</tr>
</tbody>
</table>
• **Vulnerability scanner:**
  - in particular for **web applications**, zero-day/fuzzing, consideration of **data bases**, traffic/network **analyser**, **program code** scanner

• **Penetration tester**, e.g. “SQL injection”

• **Intrusion** **detection** tools

• **Load** test/Scalability

• **Further utilities:** Model-based testing (UML testing profile) and risk modelling
TESTLAB (TESTING AND CERTIFICATION)

• Focus on open source test tools (Eclipse)
• Support of test suites configuration
• Providing several end devices
• Remote test service (online)

Future certification
  – „light weight“ selection of criteria
  – „self certification“ if tests are successful
  – consideration of operational phase
  – use of standardized test purpose catalogs (in preparation at ETSI)
SUMMARY AND OUTLOOK

What comes next?
APPROACH

✓ Advanced + mature testing technology: TTCN-3

✓ (open source) community: Eclipse

✓ Standardized basis (for certification): ETSI
New Working Group (TST) will develop IoT test catalogues and specifications (not covered elsewhere).

The types of testing include conformance, interoperability, security and performance testing.

The initial technical focus will be:
- IoT network layer (communication protocols, node connectivity, edge computing etc.),
- IoT layer (data accumulation and aggregation),
- Application layer (interfaces, business processes etc.).
APPROACH

✓ Advanced testing technology:

✓ (Open source) IoT-Testware (code):

✓ Standardized IoT test purposes:

✓ Certified Professionals for IoT
IOT QUALITY ENGINEERING

• ASQF/GTB Certified Professional for IoT Foundation Level
• New syllabus for 3-day lectures

QUALITY ENGINEERING FOR THE INTERNET OF THINKS (IOT-QE)

1) Motivation/challenges
2) Constructive QE – Quality characteristics
3) Constructive QE – IoT architecture
4) Constructive QE – Processes and methods
5) Analytic QE (incl. testing)
6) Lifecycle
Thank you for your attention!

https://www.fokus.fraunhofer.de/sqc